

CODEC NET

Security Operations Center

Monthly Report

Codec Networks Pvt. Ltd.

Executive Summary

Report Period: September 25, 2025 - October 25, 2025

Top 10 Security Alerts

Page 2 of 6

#	Severity	Alert Description	Host/Agent	Count	Last Seen
1	Critical	high-severity alert: Server resource utilization spiked unusually, possible DoS activity in progress.	wazuh-virtual-machine	114	10/14/25 12:48 PM
2	Critical	DNS request to C2 domain observed.	wazuh-virtual-machine	72	10/14/25 1:04 PM
3	Critical	high-severity Brute-force login attempts detected.	wazuh-virtual-machine	57	10/14/25 12:56 PM
4	Major	Possible kernel level rootkit	wazuh-virtual-machine	2	10/07/25 11:08 AM

Alert Statistics & Trends

Page 3 of 6

Alert Distribution

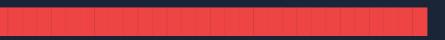
Critical **243**

Major **2**

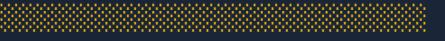
Minor **0**

Total Alerts **245**

Alert Severity Breakdown

Critical:  243

Major:  2

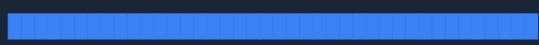
Minor:  0

Critical: 99.2% | Major: 0.8% | Minor: 0%

Daily Alert Trend (Last 7 Days)

Fri, 9/26:  1

Tue, 10/7:  1

Tue,
10/14:  243

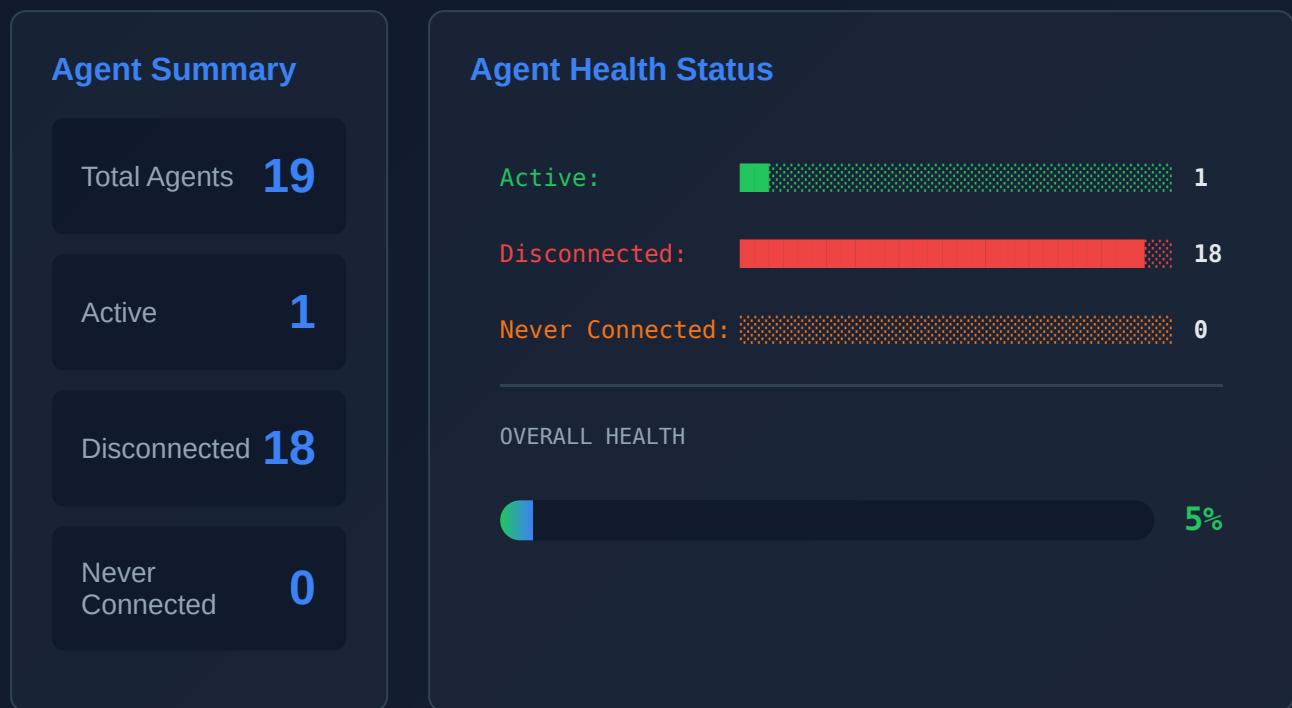
Top 5 Alert Types

High Alerts custom **243**

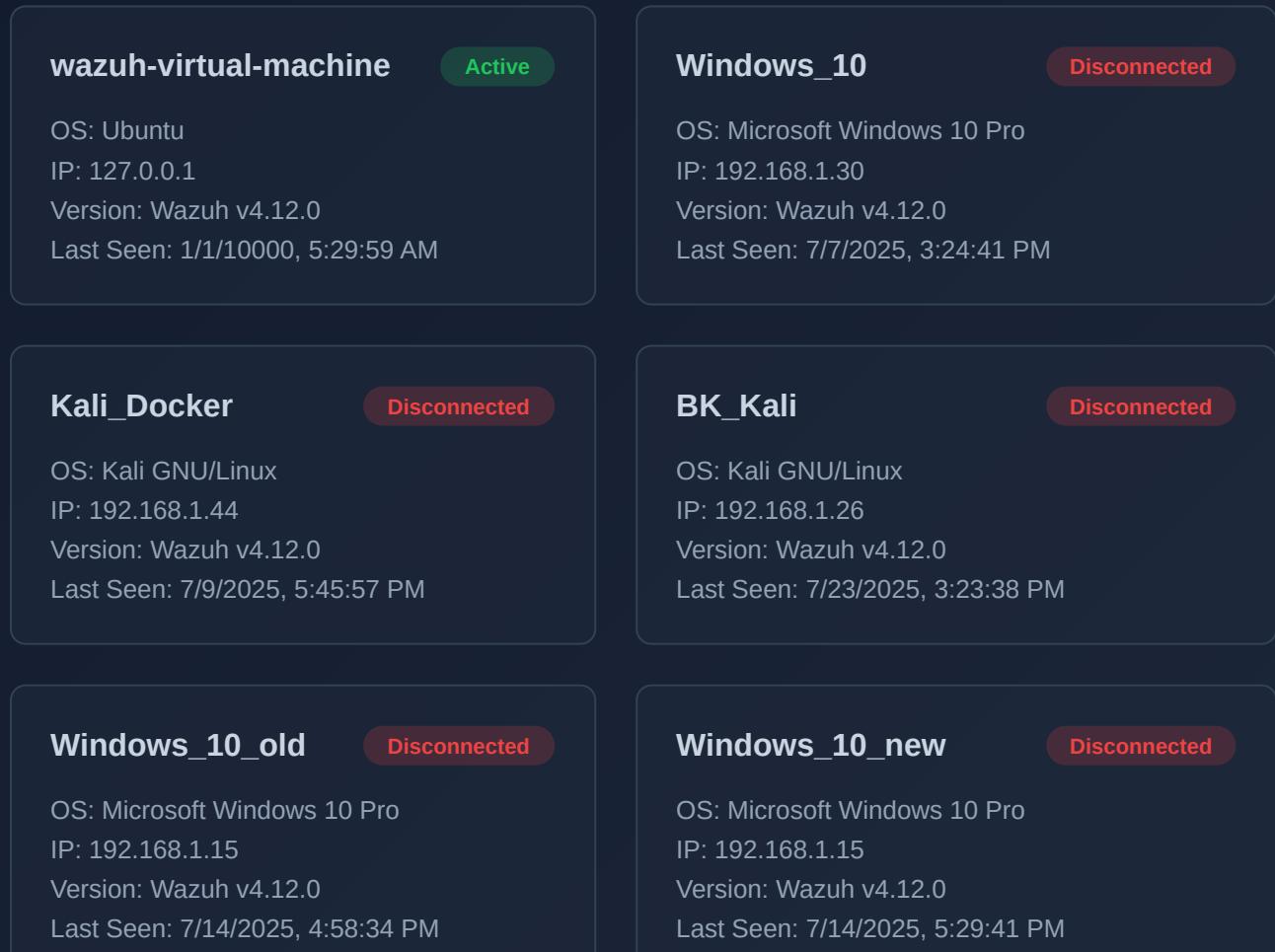
ossec **2**

Agent Status Overview

Page 4 of 6



Agent Details



OS: Kali GNU/Linux

IP: 192.168.174.128

Version: Wazuh v4.12.0

Last Seen: 8/30/2025, 2:26:00 PM

OS: Microsoft Windows 10 Pro

IP: 192.168.1.11

Version: Wazuh v4.12.0

Last Seen: 9/10/2025, 5:25:47 PM

CIS Compliance Status

Page 5 of 6

Overall Compliance Score

36%

Security Configuration Assessment - Per Policy

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 (773 passed, 1567 failed)

33%

CIS Microsoft Windows Server 2025 Benchmark (456 passed, 978 failed) **32%**

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0. (412 passed, 530 failed) **44%**

CIS Distribution Independent Linux Benchmark v2.0.0. (256 passed, 294 failed) **47%**

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0. (100 passed, 145 failed) **41%**

Agent Compliance Scores

1. BK_Kali

87 passed, 97 failed (1 policies)

47%

2. BK_Kali_new

87 passed, 97 failed (1 policies)

47%

45%



33%

16. Windows_10_quarantine

127 passed, 263 failed (1 policies)

33%

17. test_windows_all

128 passed, 262 failed (1 policies)

27%

18. mmadpay1

96 passed, 262 failed (1 policies)

27%

19. mmadpay2

96 passed, 262 failed (1 policies)

Configuration Findings Summary

Total Checks

5511

Passed

1997

Failed

3514

Overview

During the reporting period of September 25, 2025 - October 25, 2025, our Security Operations Center monitored and analyzed 245 security alerts across your infrastructure. The alert distribution shows 243 critical alerts, 2 major alerts, and 0 minor alerts.

Our team has been actively monitoring, triaging, and responding to security events in real-time. 19 agents are deployed across your infrastructure, with 1 currently active.

Security configuration assessment shows an overall compliance score of 36% with 3514 failed checks requiring attention.

